【Drawing】

【Fig. 1】

MSB-first Multiplication Algorithm Over GF(2^m)

Input : $A(x)$, $B(x)$, $G(x)$
Output : $P(x)=A(x)B(x)$ *mod* $G(x)$
1. $p_k^{(0)}=0$, for $0 \le k \le m-1$
2. $p_{-1}^{(i)}=0$, for $1 \le i \le m$
3. for i = 1 to m do
4. for $k = m-1$ to 0 do
5. $p_k^{(i)}=p_{m-1}^{(i-1)}g_k+b_{m-i}a_k+p_{k-1}^{(i-1)}$
6. end
7. end
8. $P(x) = p^m(x)$

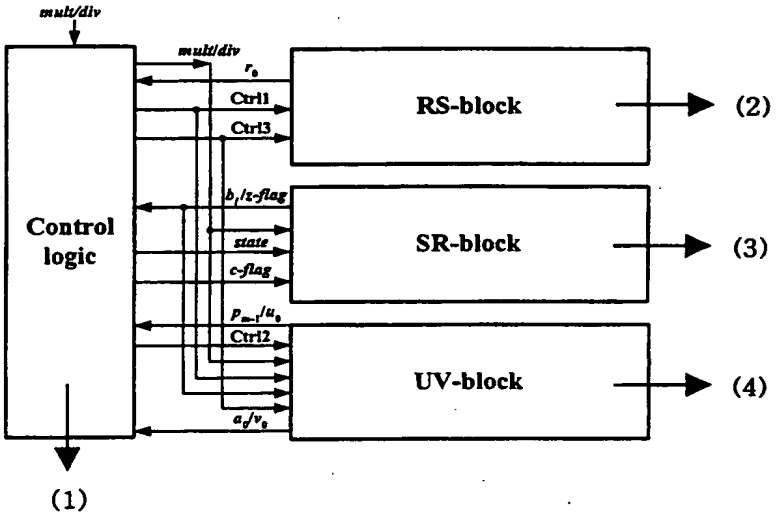
【Fig. 2】

Division Algorithm Over GF(2^m)

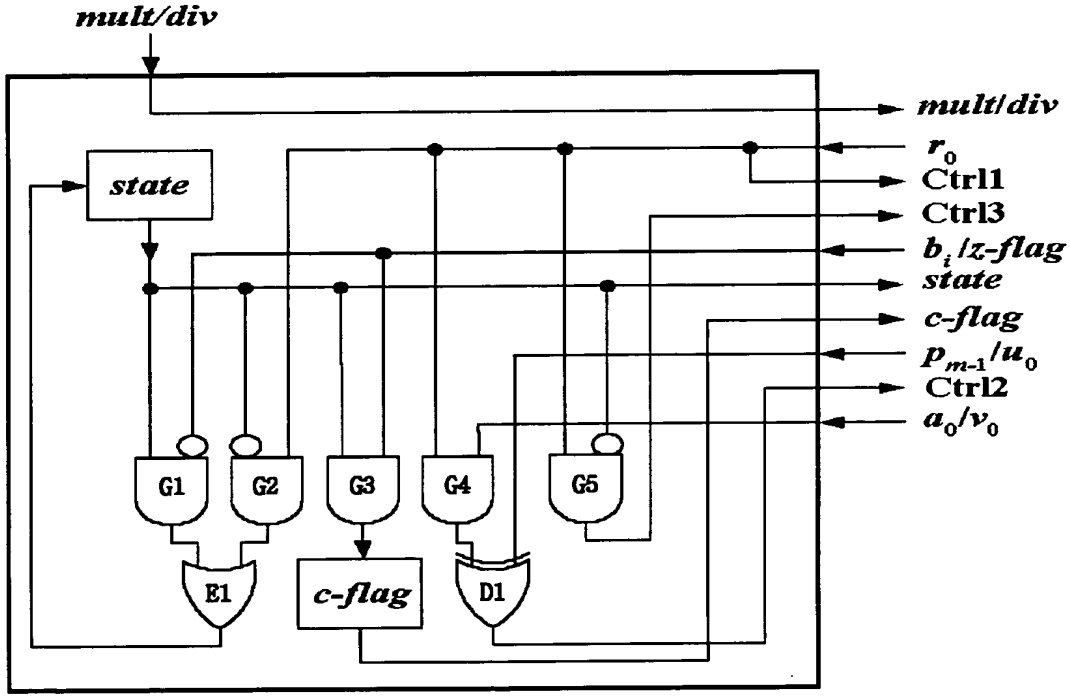
Input: $G(x)$, $A(x)$, $B(x)$
Output: V has $P(x)=A(x)/B(x)$ mod $G(x)$
Initialize: $R=B(x)$, $S=G=G(x)$, $U=A(x)$, $V=0$, *count*=0, *state*=0

1. **for** i = 1 **to** $2m$ **do**
2. **if** *state* == 0 **then**
3. *count* = *count*+1;
4. **if** r_0 == 1 **then**
5. $(S, R)=(R, R+S)$; $(V, U)=(U, U+V)$;
6. *state* = 1;
7. **end if**
8. **else**
9. *count* = *count*-1;
10. **if** r_0 == 1 **then**
11. $(S, R)=(S, R+S)$; $(V, U)=(V, U+V)$;
12. **end if**
13. **if** *count* == 0 **then**
14. *state* = 0;
15. **end if**
16. **end if**
17. $R = R/x$;
18. **if** u_0 == 0 **then**
19. $U = U/x$;
20. **else**
21. $U = (U+G)/x$;
22. **end if**
23. **end for**

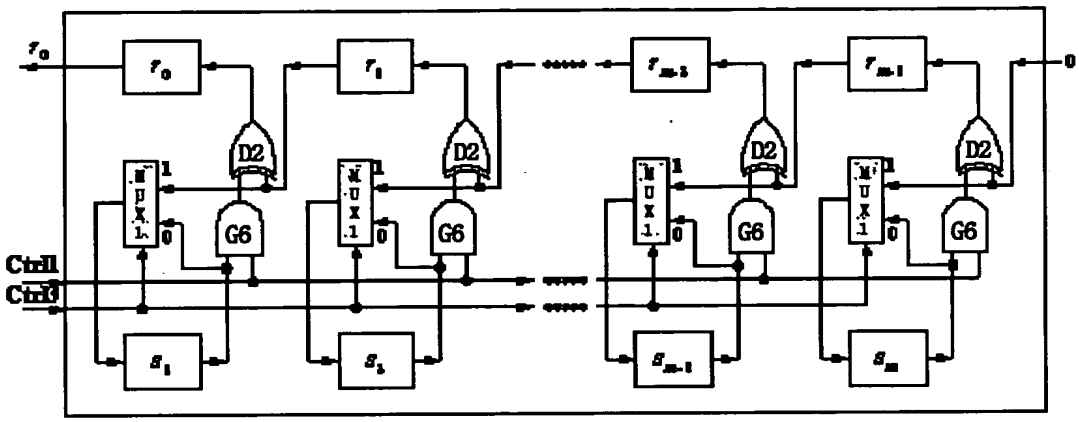
【Fig. 3】


mult/div
mult/div
r_0
Ctrl1
Ctrl3
RS-block
(2)
b_i/z-flag
state
c-flag
SR-block
(3)
Control logic
p_{m-1}/u_0
Ctrl2
UV-block
(4)
a_0/v_0
(1)

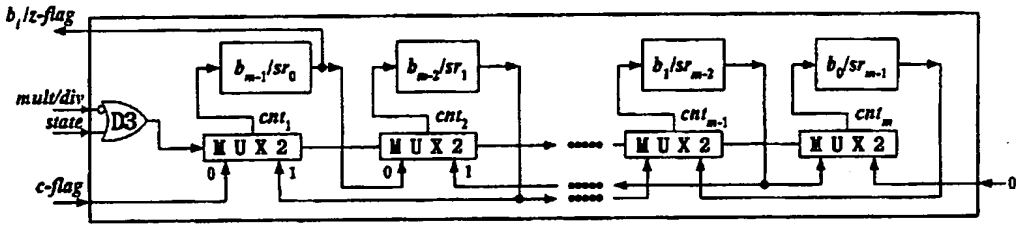
【Fig. 4】


mult/div
state
G1
G2
G3
G4
G5
E1
c-flag
D1
mult/div
r_0
Ctrl1
Ctrl3
b_i/z-flag
state
c-flag
p_{m-1}/u_0
Ctrl2
a_0/v_0

【Fig. 5】



【Fig. 6】



【Fig. 7】